Source of Acquisition
NASA Marshall Space Flight Center

IMPORTANCE OF QUALITY CONTROL IN REDUCING SYSTEM RISK, A LEASON LEARNED FROM THE SHUTTLE AND A RECOMMENDATION FOR FUTURE LAUNCH VEHICLES

Fayssal M. Safie Ph. D.
/Marshall Space Flight Center

Bradley P. Messer
/Marshall Space Flight Center

ABSTRACT

This paper presents lessons learned from the Space Shuttle return to flight experience and the importance of these lessons learned in the development of new the NASA Crew Launch Vehicle (CLV). Specifically, the paper discusses the relationship between process control and system risk, and the importance of process control in improving space vehicle flight safety. It uses the External Tank (ET) Thermal Protection System (TPS) experience and lessons learned from the redesign and process enhancement activities performed in preparation for Return to Flight after the Columbia accident. The paper also, discusses in some details, the Probabilistic engineering physics based risk assessment performed by the Shuttle program to evaluate the impact of TPS failure on system risk and the application of the methodology to the CLV.

INTRODUCTION

In the past, space vehicle designers focused more on performance and less on other system parameters. Reliability and safety was covered by designing for high safety factors. Safety factors are good if processes are in control and engineering analyses are bounding. However, past experience has shown that even for the best design, engineering analyses are not bounding in cases of excessive process variability and lack of process control. Designing and building a safe and reliable space vehicle involves good design and good manufacturing. In other words "design it right and build it right". Quality control, and more specifically process control is the key for "building it right". Additionally, process control is critical for performing adequate and bounding engineering analysis for design certification, and a key for a valid and bounding system risk assessment. Lack of process control could lead to reduced quality which leads to lower reliability and higher system risk. The Space Shuttle has experienced some of those cases, but has overcome these difficulties through extensive redesign efforts and process enhancements. The most recent example is the Space Shuttle External Tank (ET) Thermal Protection System (TPS) reliability issues that contributed to the Columbia accident. The TPS is a foam type material applied to ET to maintain cryogenic propellant quality, minimizes ice/frost formation, and protects the structure from ascent, plume, and re-entry heating. Figure 1 shows the main ET components that have TPS foam sprayed by automated or manual processes. Due to the Columbia accident, some TPS manually sprayed components were enhanced or redesigned to reduce defects. A type of defect of main concern, which was the focus of the return to flight (RTF) activities, was the presence of voids within the TPS foam. Figure 2 shows the enhanced/redesigned manually applied TPS components.

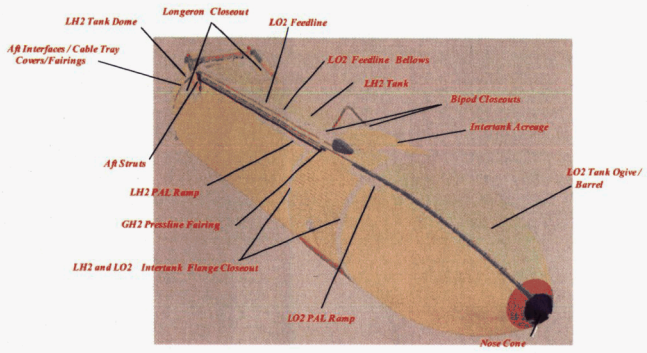

Figure 1. ET Main Thermal Protection System

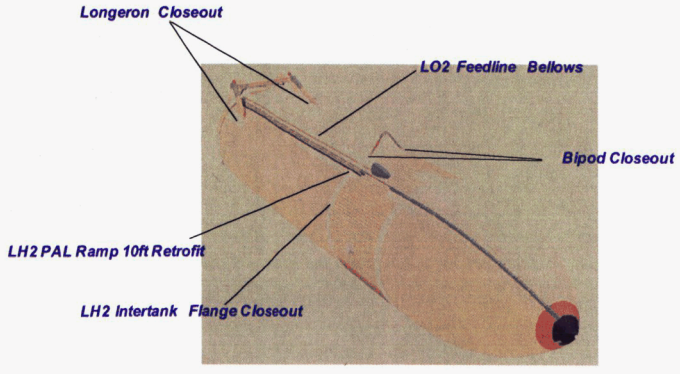

Figure 2. Enhanced/Redesigned ET Parts

ET RETURN TO FLIGHT LESSONS LEARNED

The following sections discuss the lessons learned from ET Return to Flight (RTF) with regard to process control and its impact on TPS reliability and Space Shuttle risk. The next section addresses the relationship between process control, reliability, and system risk. The rest of the sections address specific experiences from ET RTF.

Relationship between Process Control, Reliability, and System Risk

Quality engineering, and more specifically ET TPS process control is a critical factor in reducing the Space Shuttle system risk. Good process control for ET TPS translates to a lower number of defects and smaller defect sizes, which in turn, translates to a lower number of divots and smaller divot sizes released in flight that could hit the Orbiter and cause a Space Shuttle catastrophic failure. In other words, higher TPS material quality and capability means better TPS reliability and lower Shuttle risk. Figure 3 shows the relationship between process control, reliability, and system risk. The following paragraphs discuss, in more details this relationship as applied to the ET TPS.

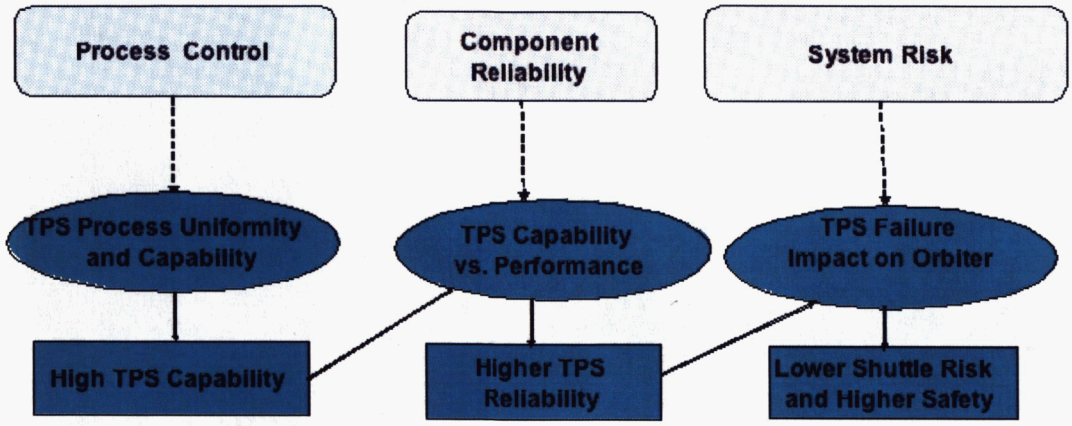

Figure 3. Relationship between Process Control, Reliability, and System Risk

We more often talk about process control in terms of statistical process control (SPC). The scope of process control is much broader than SPC. After the Columbia accident, an attempt was made by the ET project to formulate and implement an Integrated Process Control (IPC) plan for the ET TPS to ensure consistent processes were employed. As shown in Figure 4, the ET TPS IPC involved SPC, TPS application process control, manufacturing material control, contamination control, supplier process control, process change verification control, process monitoring, training and operator certification, and configuration management control. The focus of the ET project was on SPC, standardization of spray techniques, early detection of changes in materials, comprehensive technician, operator and Quality Control (QC) training, video review, process parameter data recording, and QC inspection. The ET TPS SPC activity involved identification of process factors that affect the product quality, determination of the relative magnitude of the factors and the factors' numerical sensitivity, and monitoring of the process critical factors.

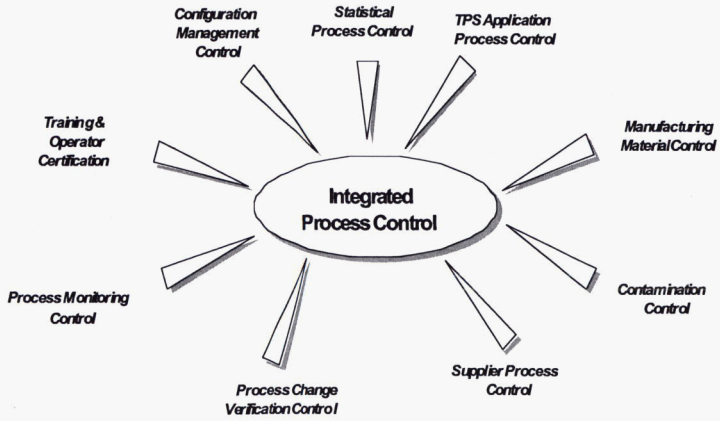

Figure 4. ET TPS Integrated Process Control

The output of ET process control was the most critical input to the TPS reliability. As shown in Figure 5, TPS reliability was defined in terms of TPS capability and system operating environment. The TPS capability was defined in terms of material properties, process uniformity, and process capability. Process uniformity and process capability were characteristic of process defect frequency and size, which were mainly driven by process control. In other words, ET TPS reliability was mainly driven by TPS process control.

The output of TPS reliability was a set of probability distributions of TPS divot frequency and divot size, which were derived from the distributions of process defect frequency and defect size taking into consideration the effect of the flight operating environment. The TPS reliability output was a critical input to the simulation model that was used to evaluate the ET TPS failure impact on the Shuttle system risk.

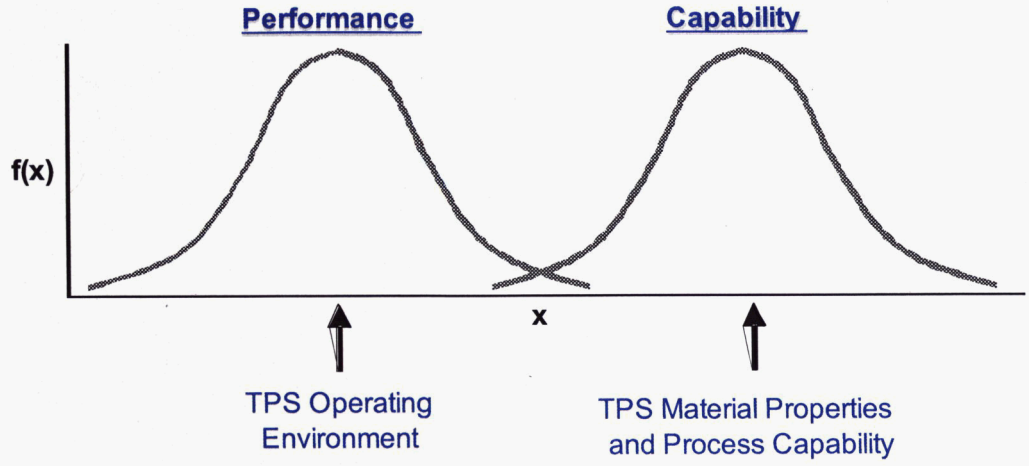

Figure 5. TPS Reliability

The following subsections address both the characterization and evaluation for redesigned/enhanced and non redesigned (Use-As-Is) TPS respectively. The section entitled "Risk Assessment" describes the process that the Shuttle program and ET project used to assess the TPS reliability and system risk using the information and data characterization generated by the effort described in this section.

Evaluation and Characterization of Redesigned ET TPS

The following section discusses the approach used for improvements and evaluations related to manually applied TPS components. Manually applied ET TPS components were improved in two different aspects; a redesign of the TPS component, and an enhancement of the manual TPS application process specific to that component. ET TPS component redesign addressed the relationship between substrate geometry and defect formation. For example, the complexity of the underlying substrate was reduced, which corresponds to a reduction in the number and size of defects induced by complex substrates. Enhancement of the manual TPS application process included considerations for reduced operator to operator variability. For example, the sequence of operations were better organized and well defined with emphasis on operator training and certification specific to an ET TPS component. This allowed for a more consistent application process.

Verification and validation testing of each TPS component redesign was performed, which provided sufficient data to evaluate and characterize the process variability and process capability. Process readiness was also evaluated using pre-control charts [4].

Statistical evaluation of the data showed that significant improvements were made in process uniformity and process capability for material properties for the enhanced/redesigned ET TPS components. Significant reduction was detected in the coefficient of variation (COV) of the process critical output parameters (e.g. density, plug pull, voids, etc.). Figure 6 shows an example of the Bipod Closeout redesign average density distribution. Furthermore, there was a significant reduction in the frequency and size of defects for the enhanced/redesigned ET TPS components. However, void characterization was still difficult because of limitation of the data and lack of good definition of the right tail of the data distribution [5].

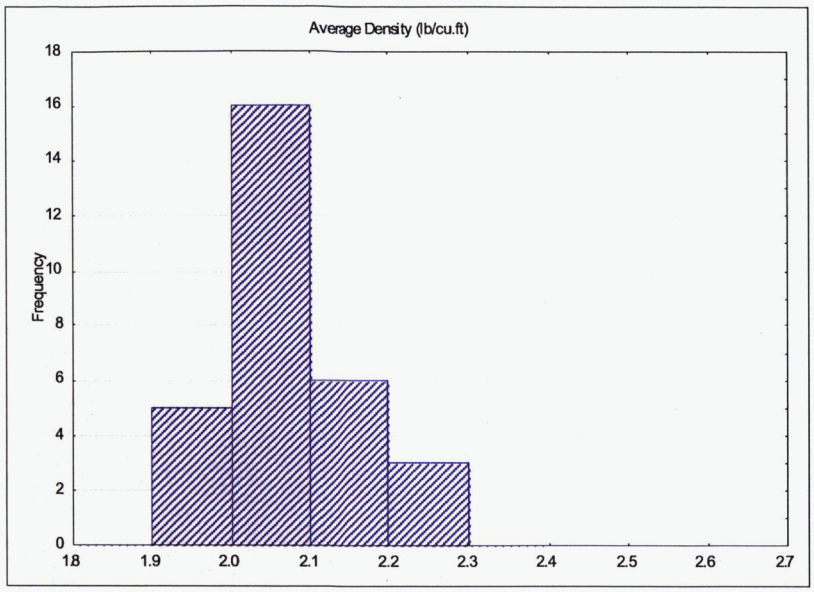

Figure 6. Example: Bipod Final Closeout Average Density

Evaluation and Characterization of Use-As-Is TPS

Process variability for Use-As-Is foam was evaluated after the fact, without complete information about process variation and controls. In other words, the natural variation of the process was not well understood, and the relationship between process control variables and defects was not known.

The dissection data collected after the Columbia accident showed excessive variability (COV is greater than 100%) for process defect sizes and frequency. Within tank defect variability was high, and tank to tank defect variability could not be fully characterized due to limited data. Defect/void characterization was difficult and statistics derived had a high level of uncertainty. There was also a lack of random samples of sufficient size to empirically select a distribution for characterization. Furthermore, there was no engineering rationale to pick a specific distribution and the data were very limited to characterize the right tail of the distribution [6].

As a result of the above process control unknowns and data limitations, statistics was used only as supporting data for engineering evaluation and analysis. Additionally, engineering factors were used in the derivation of certification limits as a penalty to compensate for the lack of complete understanding of process controls and the statistical limitations of the data.

Risk Assessment

The TPS failure impact on Shuttle risk was evaluated using a probabilistic physics based engineering approach [1] [2]. While traditional probabilistic risk assessment (PRA) involves all the scenarios that impact the system risk [3], the TPS probabilistic physics based engineering risk assessment simulation model focused on the impact of a failure mode on the system risk. It is important to note that in a traditional PRA, judgment and error factors (the ratio of the 95th percentile to the 50th percentile) are extensively used in determining the uncertainty in the risk numbers, while in an engineering physics based risk assessment, the uncertainty evaluation is mainly driven by engineering data and engineering assumptions.

The authors of this paper do not mean to indicate that traditional PRA can not be done using physics based approach. However, economically and practically speaking, only selected failure modes in a system PRA can be done using physics based approach. This is because physics based probabilistic risk assessments require extensive engineering information and extensive engineering models that are costly in nature, and as a result, their use should be limited to those complex and high risk failure modes.

The section entitled "Traditional PRA" briefly discusses the general PRA approach, while the section entitled "ET TPS Physics Based Risk Assessment" discusses in the ET TPS physics based approach.

Traditional PRA

PRA is a rigorous method to model what can go wrong with a system, predict how often it might go wrong (the probability that specific undesired events will occur), identify the consequences if something does go wrong, and, engage the design and development community to the fullest extent. PRA provides information on the uncertainty of the predictions and identifies which failures and, therefore, which systems, subsystems, and components, pose the most significant risk to the system.

Figure 7 shows a generic PRA process. The master logic diagram (MLD) is a hierarchical, top-down display of initiating events (IE), showing general types of undesired events at the top, proceeding to increasingly detailed event descriptions at lower tiers, and displaying initiating events at the bottom. The modeling of each accident scenario proceeds with inductive logic tools called event sequence diagrams (ESDs). An ESD starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events called pivotal events, until an end state is reached. ESDs are mapped into event trees (ETs), which relate more directly to practical quantification of accident scenarios, but the ESD representation has the significant advantage over the ETs of enhancing communication between risk engineers, designers, and crews. Upon completion of the event trees, Fault Trees (FTs) are created to model how failures and other events combine to cause failures of pivotal events (intermediate events) in the accident scenario. The pivotal events are placed at the tops of the FTs and deductive logic is used to identify the combination of events that may result in the top event—i.e., to develop the branches of the fault trees. The fault trees may consist of: the top event (pivotal event), intermediate events or logic gates, and the basic events. The basic events are linked to the top event through the intermediate logic gates. The fault trees are simplified through Boolean reduction to quantify each pivotal event in the scenario. The accident sequences (event sequences) and FTs are logically linked and quantified, usually using an integrated PRA computer program. The frequency of occurrence of each end state in the ET is calculated as the product of the IE frequency and the (conditional) probabilities of the pivotal events along the scenario path linking the IE to the end state. Scenarios are grouped according to the end state of the scenario defining the consequence. All end states are then grouped, i.e., their frequencies are summed up into the frequency of a representative end state. As part of the quantification, uncertainty analyses are performed to evaluate the degree of knowledge or confidence in the calculated numerical risk results. [7]

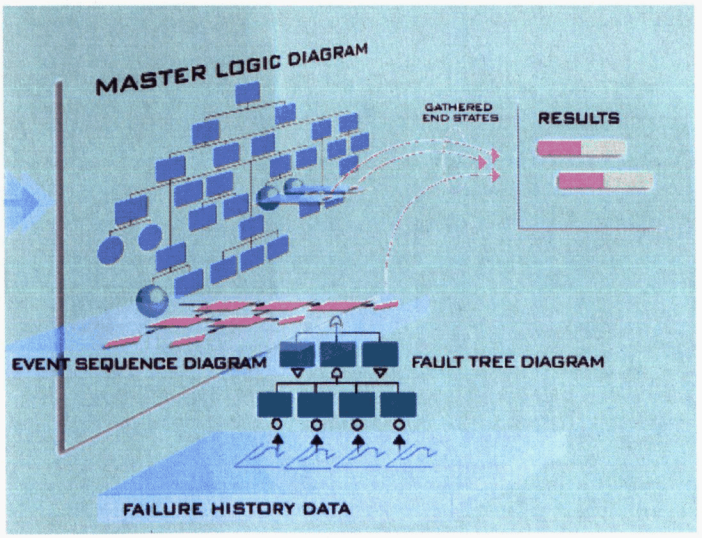

Figure 7. PRA Process

ET TPS Physics Based Risk Assessment

The Shuttle Program identified and categorized all potential ET TPS debris sources in order to assess the risk to the Shuttle Orbiter. As mentioned earlier, the impact of an ET TPS failure on Shuttle risk was evaluated using a physics based probabilistic engineering simulation approach. The risk assessment model, although limited in scope, was very critical in understanding and communicating the risk derived from the loss of ET TPS in flight. Estimates

of the risk numbers and the level of confidence are heavily dependent on the level of conservatism of the engineering data and engineering assumptions. To date these conservatisms have not been driven out of the simulation due to modeling limitations, limited test data and a lack of time.

The Space Shuttle ET TPS risk assessment approach as shown in Figure 8, consists of a five part probabilistic Monte Carlo physics-based simulation model. The first part of the simulation model is used to characterize ET TPS internal voids using the ET TPS void distributions. The main input to the simulation model was the ET TPS void distributions derived from the dissection data of the ET components under consideration. The second part of the simulation model is TPS debris generation and release. The TPS void distributions were input into a fracture mechanics model based on the physics of TPS. Divot size, shape, time of release, and pop-off velocity is generated. The divots generated in the physics based fracture mechanics model are then transported from the ET toward the Orbiter in the third part of the assessment. Whether a specific piece of liberated ET TPS hits the Orbiter is determined in the fourth segment of the simulation. If the liberated ET TPS is deemed to strike the Orbiter, an impact location, time, mass, velocity, and angle of impact is then generated. The final segment of the simulation is the Orbiter damage assessment. The final output of the simulation model is the probability of Orbiter damage exceeding a specified tolerance limit set for the Orbiter reentry survivability.

As described above the simulation model is used to predict expected ET TPS liberation events, transport and impact damage. The results of the simulations are used to develop flight rational and to support near-real time analysis of witnessed damage during future Shuttle missions. Each piece of the simulation model offers unique strengths and provides significant improvement above the pre-*Columbia* capabilities. It is important to note that the void distributions represent the output of the ET TPS manual application process, which was basically driven by process control.

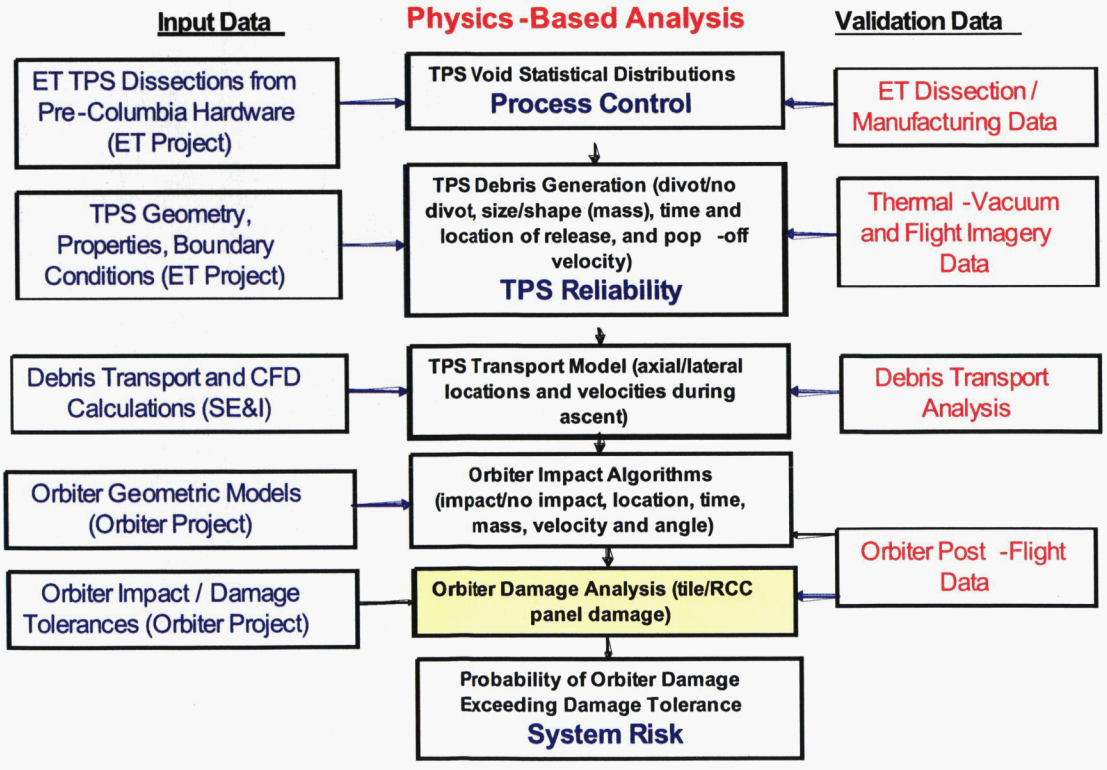

Figure 8. Shuttle ET TPS Risk Assessment Approach

IMPORTANCE OF SHUTTLE LESSONS LEARNED FOR THE NASA CREW LAUNCH VEHICLE (CLV) PROGRAM

NASA is in the process of developing a new launch vehicle to replace the Space Shuttle. The new launch vehicle, called the CLV, is targeting an ambitious safety goal of an order of magnitude better than the existing

Shuttle. Using the lessons learned from ET RTF, the CLV program needs to emphasize two major areas addressed in this paper. The first area is process control, and the second area is PRA. With regard to process control, the CLV program should consider manufacturing and quality control upfront in the design process. Specifically, an integrated process control plan similar to one discussed earlier, should be put in place upfront and implemented though out the various phases of the CLV program. With regard to PRA, the CLV program should implement a structured PRA process supported with an engineering physics based analysis approach to assess system risk, and at the same time optimize the system reliability and system safety. In other word, the CLV program should use the traditional PRA system approach as a frame of work to identify the system failure scenarios and emphasize those areas where physic based in depth engineering modeling is required to help designers to minimize the risk of the failure modes that are complex in nature and have a major impact on the overall system risk.

CONCLUSION

Lessons learned from ET RTF experience demonstrated that a minor problem in process control could lead to a major problem at the system level which could significantly impact system risk. Consequently, good process control is essential in achieving high component reliability and low system risk. Manufacturing and process control should be considered up front in designing future space launch vehicles. Component designers should consider manufacturability as well as the feasibility of good process control in their design selection process. Finally, to ensure consideration of process control early on, an integrated process control plan should be developed upfront, and implemented throughout the different phases of future programs.

Additionally, Shuttle lessons learned showed the need for component designer to perform a probabilistic physics based engineering analysis for those complex failure modes that might have a major impact on the overall system risk. This type of analysis need to be identified, planned, integrated in the program schedule, and performed upfront in the design phase and throughout the other phases of the program as necessary.

ACKNOWLEDGMENTS

The authors would like to acknowledge the contribution of Mr. Son Nguyen, of Lockheed Martin Space System Company as well as the contribution and support of the ET project office at Marshall Space Flight Center in Huntsville, Alabama, and the ET RTF team at Lockheed Martin Space Company at Michoud Operation, New Orleans.

REFERENCES

[1] Safie F. M., 1991, "A Probabilistic Design Analysis Approach for Launch Systems," AIAA 27th Joint Propulsion Conference, Sacramento, CA, USA.

[2] Safie F. M., 1992, "Use of Probabilistic Design Methods for NASA Applications," ASME Symposium on Reliability Technology, Anaheim, CA.

[3] Safie F. M., 1998, "An Overview of Quantitative Risk Assessment for the Space Shuttle Propulsion Elements," The Fourth Probabilistic Safety Assessment and Management (PSAM4), NY City, NY.

[4] Bhote K. and Bhote A., 2000, "World Class Quality: Using Design of Experiments to Make it Happen," Amacom, New York, New York, USA.

[5] Nguyen S. C., 2005, "Enhanced TPS Evaluation Data Update, Lockheed Martin Memorandum 4200-05-007," New Orleans, Louisiana, USA.

[6] Kelly M. A., 2004, "As Built Dissection Data Statistical Analysis, Lockheed Martin Memorandum 4210-04-024," New Orleans, Louisiana, USA.

[7] NPR 8705.5, Probabilistic Risk Assessments (PRA) Procedures for NASA Programs and Projects